THABA CHWEU MUNICIPALITY

Disaster Recovery Plan

Methodology

Document Name	TCM_Disaster Recovery Plan_v1.2.pdf
Document Version	1.1
Client Version	1.2
Approved Date	
Last Reviewed By	ICT Review Team
Last Reviewed Date	

After a significant business disruption, the Municipality's goal is to recover and resume business operations as quickly as possible, while safeguarding their employees and property; protecting information assets, and to commence with service delivery to its clients both internally and externally. This Disaster recovery plan is developed to govern the processes and procedures that must be followed to resume operations as quickly as possible, given the scope and severity of the significant business disruption.


RE DIRELA BATHO

Table of Contents

Document Reference 3
1 Overview 4
2 Objective 4
3 Scope 4
4 Methodology 5
4.1 Phase 1 - Pre-Planning Activities (Project Initiation) 5
4.2 Phase 2 - Vulnerability Assessment and General Definition of Requirements 5
4.3 Phase 3 - Business Impact Assessment (BIA) 6
4.4 Phase 4 - Detailed Definition of Requirements 6
4.5 Phase 5 - Plan Development 6
4.6 Phase 6 – Testing and Exercising Program 7
4.7 Phase 7 - Maintenance Program 7
4.8 Phase 8 - Initial Plan Testing and Implementation 7
5 PROGRAM DESCRIPTION 7
5.1 Planning scope and plan objectives 7
5.2 Project organization and staffing 8
5.3 Steering Committee 9
5.4 Project Team 9
5.5 Suggested Information Systems and Technology support team Composition 9
6 Project Control 10
7 Schedule of Deliverables 10
8 Resource Requirements 11
9 Corrective actions for non-policy compliance 11
10 Glossary and Abbreviations 112

Document Reference

Author (Version 1.0)			
Date	**Name**	**E-mail**	**Contact**
August 2012	Johann Wiese	johann.wiese@ gmail.com	+27 79 786 9132

Contributors			
Version	**Name**	**E-mail**	**Contact**
1.2	Sbusiso Langa	langa@ thabacweumun.gov.za	+27 13 235 7365 +27 73 237 8488

Review Team			
Version	**Name**	**E-mail**	**Contact**
1.2	Gareth Mnisi	gmnisi@ thabachweumun.gov.za	+27 13 235 7372 +27 71 624 8127
	Surprise Maebela	smaebela@ thabachweumun.gov.za	+27 13 235 7304 +27 79 871 8627
	Senty Mokgohloa	senty@ thabachweumun.gov.za	+27 13 235 7365 +27 78 599 9125
	Thapelo Ngwatle	thaphelo@ thabachweumun.gov.za	+27 13 235 7566 +27 84 611 1904

Change Record			
Version	**Date**	**Name**	**Reference**
1.1		Johann Wiese	Add client information
1.2		Sbusiso Langa	Final changes to client information

1 Overview

Historically, the data processing function alone has been assigned the responsibility for providing a business contingency plan. This has led to the development of recovery plans to restore computer resources in a manner that is not fully responsive to the needs of the business supported by those resources. Contingency planning is a business issue rather than a data processing issue. In the Municipality's environment, the effects of long-term operations outage may have a catastrophic impact on the service delivery of the Municipality. The continuous development and improvement of a viable business continuity plans and a data restore strategies must be one of the key business objective of the Thaba Chweu Municipality.

2 Objective

The primary objective of a Disaster Recovery Plan is to enable the Municipality to survive a data disaster and to re-establish normal business operations. In order to survive, the Municipality must ensure that critical operations can resume normal processing within a reasonable time frame.

3 Scope

The following process shall be used to develop the Thaba Chweu Municipality's Business Continuity plan, emphasizes the following key aspects:

- Providing management with a comprehensive understanding of the total effort required to develop and maintain an effective data recovery and restore plan;
- Obtaining commitment from senior management to support and participate in the effort;
- Defining recovery and restore requirements from the perspective of business functions;
- Documenting the impact of an extended loss of operations and key business functions;
- Focusing appropriately on disaster prevention and impact minimization, as well as orderly recovery;
- Selecting project teams that ensure the proper balance required for plan development;
- Developing a contingency plan that is understandable, easy to use and easy to maintain; and
- Defining how contingency planning considerations must be integrated into on-going business planning and system development processes in order for the plan to remain viable over time.

4 Methodology

Data recovery and restore planning is a very complex and labour intensive process; it therefore requires redirection of valuable technical staff and information processing resources as well as appropriate funding. In order to minimize the impact such an undertaking would have on scarce resources, the project for the development and implementation of disaster recovery and business resumption plans should be part of the organization's normal planning activities.

4.1 Phase 1 - Pre-Planning Activities (Project Initiation)

Phase 1 is used to obtain an understanding of the existing and projected computing environment of the organization. This enables the project team to:

- Refine the scope of the project and the associated work program.
- Develop project schedules.
- Identify and address any issues that could have an impact on the delivery and the success of the project.

During this phase a Steering Committee should be established. The committee should have the overall responsibility for providing direction and guidance to the Project Team. The committee should also make all decisions related to the recovery planning effort. The Project Manager should work with the Steering Committee in finalizing the detailed work plan.

Two other key deliverables of this phase are:

- The development of a policy to support the recovery programs and;
- An awareness program to educate management and senior individuals who will be required to participate in the project.

4.2 Phase 2 - Vulnerability Assessment and General Definition of Requirements

Security and control within an organization is an on-going concern. It is preferable, from a business strategy perspective to concentrate on activities that have the effect of reducing the possibility of disaster occurrence, rather than concentrating primarily on minimizing impact of an actual disaster. This phase addresses measures to reduce the probability of occurrence.

This phase will include the following key tasks:

- A thorough Security Assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration; application controls; and personal computers.

- The Security Assessment will enable the project team to implement required emergency plans and disaster prevention measures where none exist.
- Present findings and recommendations resulting from the activities of the Security Assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.
- Define the scope of the planning effort.
- Analyse, recommend and purchase recovery, restore and maintenance software required to support the development of the plans and to maintain the plans current following implementation.
- Develop a Plan Framework.

4.3 Phase 3 - Business Impact Assessment (BIA)

A Business Impact Assessment (BIA) of all business units that are part of the business environment enables the project team to:

- Identify critical systems, processes and functions
- Assess the economic impact of incidents and disasters that result in a denial of access to systems services and other services and facilities and
- Assess the "pain threshold," that is, the length of time business units can survive without access to systems, services and facilities.
- The BIA Report should be presented to the Steering Committee. This report identifies critical service functions and the timeframes in which they must be recovered after interruption. The BIA Report should then be used as a basis for identifying systems and resources required to support the critical services provided by information processing and other services and facilities.

4.4 Phase 4 - Detailed Definition of Requirements

During this phase, a profile of recovery requirements is developed. This profile is to be used as a basis for analysing alternative recovery and restore strategies. The profile is developed by identifying resources required to support critical functions identified in Phase 3. This profile should include hardware (Servers, data and communications and personal computers), software (vendor supplied, in-house developed, etc.), documentation (DP, user, procedures), outside support (public networks, DP services, etc.) and facilities (office space, office equipment, etc.) Another key deliverable of this phase is the definition of the plan scope, objectives and assumptions.

4.5 Phase 5 - Plan Development

During this phase, recovery and restore plan components are defined and plans are documented. This phase also includes the implementation of changes to user procedures, upgrading of existing data processing operating procedures required to support selected recovery strategies and alternatives, vendor contract negotiations (with suppliers of recovery services) and the definition of Recovery and Restore Teams, their roles and responsibilities. Recovery and Restore standards are also to be developed during this phase.

4.6 Phase 6 – Testing and Exercising Program

The plan Testing and Exercising Program is developed during this phase. Testing and exercising goals are established and alternative testing strategies are evaluated. Testing strategies tailored to the environment should be selected and an on-going testing program should be established.

4.7 Phase 7 - Maintenance Program

Maintenance of the plans is critical to the success of an actual recovery. The plans must reflect changes to the environments that are supported by the plans. It is critical that existing change management processes are revised to take recovery plan maintenance into account. In areas where change management does not exist, change management procedures will be recommended and implemented.

4.8 Phase 8 - Initial Plan Testing and Implementation

Once plans are developed, initial tests of the plans are conducted and any necessary modifications to the plans are made based on an analysis of the test results.

Specific activities of this phase include the following:

- Defining the test purpose and approach.
- Identifying test teams.
- Structuring the test.
- Conducting the test.
- Analysing test results.
- Modifying the plans as appropriate.

The approaches taken to test the plans depend in large part on the recovery and restore strategies selected to meet the requirements of the organization. As the recovery and restore strategies are defined, specific testing procedures should be developed to ensure that the written plans are comprehensive and accurate.

5 PROGRAM DESCRIPTION

5.1 Planning scope and plan objectives

The primary objective of recovery planning is to enable an organization to survive a disaster and to continue normal business operations. In order to survive, the organization must assure that critical operations can resume and continue normal processing. Throughout the recovery effort, the plan establishes clear lines of authority and prioritizes work efforts. The key objectives of the contingency plan should be to:

- Continue critical business operations
- Minimize the duration of a serious disruption to operations and resources (both information processing and other resources)
- Minimize immediate damage and losses
- Establish management succession and emergency powers
- Facilitate effective co-ordination of recovery tasks
- Reduce the complexity of the recovery effort
- Identify critical lines of business and supporting functions

Although statistically the probability of a major disaster is remote, the consequences of an occurrence could be catastrophic, both in terms of operational impact and public image. Management appreciates the implications of an occurrence. Therefore, it should assign on-going responsibility for recovery planning to an employee dedicated to this essential service.

Management must make a decision to undertake a project that satisfies the following objectives:

- Determine vulnerability to significant service interruptions in the Data Centre and business facilities and define preventive measures that may be taken to minimize the probability and impact of interruptions.
- Identify and analyse the economic, service, public image and other implications of extended service interruptions in the Data Centre and other business facilities.
- Determine immediate, intermediate and extended term recovery needs and resource requirements.
- Identify the alternatives and select the most cost effective approaches for providing backup operations capability and timely service restoration.
- Develop and implement contingency plans that address both immediate and longer-term needs for the Data Centre and other business facilities.

5.2 Project organization and staffing

The project team organization is designed to maximize the flexibility needed to deal with the implementation of a plan in the most efficient manner possible. As explained earlier in this document, disaster recovery and business resumption planning is a complex and labour intensive program. A key factor in the successful development and implementation of recovery and resumption programs in other organizations is the dedication of a full-time resource to recovery / business continuity planning.

Recovery and Restore plans should be treated as living documents. Both the information processing and the business environments are constantly changing and becoming more integrated and complex. Recovery plans must keep pace with these changes. Continuous testing and exercising of plans is essential if the organization wants to ensure that recovery capability is maintained in such an environment. The organization must also ensure that staff with recovery responsibilities are prepared to execute the recovery plans.

This cannot be achieved without a full-time resource with responsibility for: maintaining plans; coordinating components and full plan tests; training staff with recovery responsibilities; and updating plans to reflect changes to the information processing and business environments.

5.3 Steering Committee

The Steering Committee should include representatives from key areas of the organization:

- Information Systems
- Technology Support
- Systems Development
- Network and Operations Services

5.4 Project Team

The composition of the Project Team may vary depending on the environments and business units for which plans are developed. It is important to note that the managers of environments and business units for which plans are developed will be responsible for the maintenance and testing of their respective plans. However, the person or unit responsible for the recovery and continuity planning should retain the role of co-ordinator of testing activities, major plan revisions and maintainer of the Master Plan.

The Core Project Team is automatically part of other project teams. Internal Audit should be invited to be part of all teams. The managers represented on the various teams may choose to recommend other senior individuals in their area to represent them or to join specific teams where their expertise will be required for the development of the plans.

Suggested Core Project Team Composition

- Project Manager
- Computer and Network Operations
- Systems Support

5.5 Suggested Information Systems and Technology support team Composition

- Network & Communications
- Facilities Management
- Network Development and Support
- Database Administration
- Information Systems Security
- Operations
- Network Support
- Network Implementation

6 Project Control

The management and control for this project should be supported by project management software. The software should be used for scheduling of personnel resources to specific tasks and identification of end deliverables and their target completion dates. During Phase 1 activities, detail work plans for Data Processing and user personnel identifying tasks and responsibilities along with their associated start and completion dates will be developed.

7 Schedule of Deliverables

The following is a schedule of deliverables by phase that will be developed and delivered as part of this project.

- Phase 1 – Pre-Planning Activities (Project Initiation)
  - Revised Detail Work Plan
  - Policy Statement
  - Recovery Planning Awareness Program
- Phase 2 - Vulnerability Assessment
  - Security Assessment Report
  - Scope of Planning Effort
  - Plan Framework
- Phase 3 – Business Impact Analysis
  - Business Impact Assessment Report
- Phase 4 – Detailed Definition of Requirements
  - Recovery Needs Profile
  - Plan Scope, Objectives and Assumptions
- Phase 5 –Plan Development
  - Data Centre Recovery Plan
  - Recovery Standards
- Phase 6 – Testing Program
  - Testing Goals
  - Testing Strategies
  - Testing Procedures
- Phase 7 – Maintenance Program
  - Maintenance Procedures
  - Change Management Recommendations
- Phase 8 – Initial Plan Testing and Implementation
  - Initial Test Report
  - Implementation

8 Resource Requirements

Organizations who have tried to develop disaster and business resumption plans without dedicating the required resources to the effort have been largely unsuccessful in implementing effective recovery plans. Some organizations, after spending time and money developing recovery plans, have failed in maintaining their recovery capability. This is mostly due to a lack of commitment to keep their plans current or to do regular testing of recovery capabilities.

It is therefore essential, that management is committed to the development, implementation and maintenance of this program, that required resources are freed up during the development cycle and that a resource be dedicated to the on-going maintenance of the program.

9 Corrective actions for non-policy compliance

- Failure to comply with the guidelines stipulated in the Municipality's policies will result in the following corrective or disciplinary procedures.
- The decisive action that will be taken against the employee is dependent on the severity level and the level of the security risk.
- Warning from Management
    - The employee receives a warning from their manager that they were in violation of policy.
- Written Warning in Personnel File
    - The employee is reprimanded, and official notice is put in their personnel file. This may have negative consequences during future performance reviews or promotion considerations.
- Revoking Privileges
    - Access to certain resources, such as internet or email, can be revoked for a limited period providing that this action does not have a negative impact on the employee's job functions.
- Training
    - Adequate training to create awareness and guidance on policy compliance.
- Disciplinary action will be determined in compliance to Schedule 8 of the Labour Relations Act 66 of 1995 or other related Public Service Regulations.

10 Glossary and Abbreviations

Please refer to the Thaba Chweu Glossary and abbreviations guide.

Version Control

Version	State/Change	Author	Date
1.0	Original	Sbusiso Langa	
1.1	Changes	Sbusiso Langa	

Author

Name	Designation	Signature	Contact
Sbusiso Langa	Security Officer		+27 13 235 7367

Review

Name	Designation	signature	Date

Approval

Name	**Designation**	**Signature**	**Date**